Attorney's Docket No. 5670-26 PATENT

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re: Lineman et al
Serial No.: 09/966,006
Filed: September 28, 2001
Confirmation No. 4813
Group No.: 2131
Examiner: Christopher A. Revak
For: METHOD AND APPARATUS FOR ACTIVELY MANAGING SECURITY POLICIES FOR USERS AND COMPUTERS IN A NETWORK

Date: July 11, 2006

Mail Stop Appeal Brief-Patents
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

TRANSMITTAL OF APPEAL BRIEF
(PATENT APPLICATION--37 C.F.R. § 41.37)

1. Transmitted herewith is the APPEAL BRIEF for the above-identified application, pursuant to the Notice of Appeal filed on March 13, 2006 and the Decision from the Appeal Brief Conference mailed June 13, 2006.

2. This application is filed on behalf of
☐ a small entity.

3. Pursuant to 37 C.F.R. § 41.20(b)(2), the fee for filing the Appeal Brief is:
☐ small entity $250.00
☒ other than small entity $500.00

Appeal Brief fee due $__500.00_____

☒ Any additional fee or refund may be charged to Deposit Account 50-0220.

Respectfully submitted,

Robert W. Glatz
Registration No. 36,811

Myers Bigel Sibley & Sajovec, P.A.
P. O. Box 37428
Raleigh, North Carolina 27627
Telephone: (919) 854-1400
Facsimile: (919) 854-1401
Customer No. 20792

Certificate of Mailing under 37 CFR 1.8

I hereby certify that this correspondence is being deposited with the United States Postal Service with sufficient postage as first class mail in an envelope addressed to: Mail Stop Appeal Brief-Patents, Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450 on July 11, 2006.

Carey Gregory

AF
SFW

Attorney's Docket No. 5670-26 PATENT

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re: Lineman et al
Serial No.: 09/966,006
Filed: September 28, 2001
For: METHOD AND APPARATUS FOR ACTIVELY MANAGING SECURITY POLICIES FOR USERS AND COMPUTERS IN A NETWORK

Confirmation No. 4813
Group No.: 2131
Examiner: Christopher A. Revak

July 11, 2006

Mail Stop Appeal-Brief Patents
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

APPELLANTS' BRIEF ON APPEAL UNDER 37 C.F.R. §41.37

Sir:

This Appeal Brief is filed pursuant to the "Notice of Appeal to the Board of Patent Appeals and Interferences" mailed March 13, 2006 and the Decision from the Appeal Brief Conference mailed from the United States Patent Office on June 13, 2006.

Real Party In Interest

The real party in interest is assignee NetIQ Corporation, a Delaware corporation having its principal place of business in Houston, Texas.

Related Appeals and Interferences

Appellants are aware of no appeals or interferences that would be affected by the present appeal.

07/14/2006 TBESHAH1 00000007 09966006
01 FC:1402 500.00 OP

Status of Claims

Appellants appeal the final rejection of Claims 1-56, which as of the filing date of this Brief remain under consideration. The attached Appendix A presents the claims at issue as finally rejected in the final Office Action of December 13, 2005 (hereinafter "Final Action").

Attorney's Docket No. 5670-26 PATENT

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re: Lineman et al
Serial No.: 09/966,006
Filed: September 28, 2001
Confirmation No. 4813
Group No.: 2131
Examiner: Christopher A. Revak
For: METHOD AND APPARATUS FOR ACTIVELY MANAGING SECURITY POLICIES FOR USERS AND COMPUTERS IN A NETWORK

Mail Stop Appeal-Brief Patents
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

APPELLANTS' BRIEF ON APPEAL UNDER 37 C.F.R. §41.37

Sir:

This Appeal Brief is filed pursuant to the "Notice of Appeal to the Board of Patent Appeals and Interferences" mailed March 13, 2006 and the Decision from the Appeal Brief Conference mailed from the United States Patent Office on June 13, 2006.

Real Party In Interest

The real party in interest is assignee NetIQ Corporation, a Delaware corporation having its principal place of business in Houston, Texas.

Related Appeals and Interferences

Appellants are aware of no appeals or interferences that would be affected by the present appeal.

Status of Claims

Appellants appeal the final rejection of Claims 1-56, which as of the filing date of this Brief remain under consideration. The attached Appendix A presents the claims at issue as finally rejected in the final Office Action of December 13, 2005 (hereinafter "Final Action").

Status of Amendments

The attached Appendix A presents the pending claims and each of the pending claims corresponding status. All amendments in the present case have been entered.

Summary of the Claimed Subject Matter

The present application includes Independent Claims 1, 11, 26, and 51. The claims are method and system claims. Claim 1 is directed to methods for managing a security policy for one or more users in a network. Such methods may be provided by running a policy management program on a computer in communication with the network. *See* Specification, paragraph 15. The method further enables the creation of a security policy document in a portable representation language using the policy management program, including selection and inclusion in the security policy document of a plurality of data elements for communicating the security policy to the one or more users and of at least one data element for implementing the security policy on computer systems in the network. *See* Specification, paragraphs 40-47. The method also enables viewing the security policy document using the plurality of data elements for communicating the security policy to the one or more users included in the security policy document by the one or more users on the network. *See* Specification, paragraphs 16, 44 and 59-60. Electronic data relevant to user viewing of the security policy document is received using the policy management program. *See* Specification, paragraphs 55 and 59-62.

Independent Claim 11 is directed to methods for managing a security policy for one or more first computers in a network. Such methods may be provided by running a software program on a second computer in communication with the network. *See* Specification, paragraphs 13-15. The method further enables creation of a security policy document using the software program by enabling selection of security policies from a set of options. *See* Specification, paragraph 31. The security policy document is automatically configured to provide one or more technical controls for implementing the security policy on at least one first computer. *See* Specification, paragraph 24.

Independent Claim 26 is directed to methods for managing a security policy for one or more users and one or more first computers in a network. Such methods may be provided by running a software program on a second computer in communication with the network. *See* Specification, paragraphs 13-15. A security policy document is created using the software

program. *See* Specification, paragraph 15. The security policy document is automatically configured to create a human-readable security policy document and a machine-readable security policy document containing technical controls readable by at least one first computer. *See* Specification, paragraphs 20-21.

Independent Claim 51 is directed to a system for managing a security policy for one or more users and for one or more first computers in a network. The system includes a first device containing a first program for creating a security policy document in both human-readable and machine-readable formats. *See* Specification, paragraphs 13-15 and 20-21. The system further includes a second device in communication with the first device and containing a second program for monitoring the security compliance of at least one first computer. *See* Specification, paragraphs 8, 48, 50 and 55. In some embodiments at least one first computer contains a third program for receiving the machine-readable format of the security policy document. *See* Specification, paragraphs 24, 36-38 and 75-77.

Claim 16 includes recitations related to embodiments where detect rules are distributed to at least one first computer. *See* Specification, paragraph 25.

Claim 18 includes recitations related to embodiments where the one or more technical controls are distributed to at least one first computer. *See* Specification, paragraph 21.

Claim 19 includes recitations related to embodiments where a second software program is run on at least one first computer to allow at least one first computer to interpret the distributed technical controls. *See* Specification, paragraph 24.

Claims 53 to 56 include various recitations related to particular data elements and platform control elements for different operating platforms. *See* Specification, paragraphs 43-48.

Grounds of Rejection to Be Reviewed on Appeal

1. Claims 1-56 stand rejected under 35 U.S.C. § 102(e) as being unpatentable over United States Patent No. 6,735,701 to Jacobson (hereinafter "Jacobson").

Argument

I. Introduction

The pending claims are rejected as obvious under 35 U.S.C. § 102. Under 35 U.S.C. § 102, "a claim is anticipated only if each and every element as set forth in the claim is found,

either expressly or inherently described, in a single prior art reference." M.P.E.P. § 2131 (quoting *Verdegaal Bros. v. Union Oil Co.*, 814 F.2d 628, 631, 2 U.S.P.Q.2d 1051, 1053 (Fed. Cir. 1987)). "Anticipation under 35 U.S.C. § 102 requires the disclosure in a single piece of prior art of each and every limitation of a claimed invention." *Apple Computer Inc. v. Articulate Sys. Inc.*, 57 U.S.P.Q.2d 1057, 1061 (Fed. Cir. 2000).

A finding of anticipation further requires that there must be no difference between the claimed invention and the disclosure of the cited reference as viewed by one of ordinary skill in the art. *See Scripps Clinic & Research Foundation v. Genentech Inc.*, 18 U.S.P.Q.2d 1001 (Fed. Cir. 1991). In particular, the Court of Appeals for the Federal Circuit held that a finding of anticipation requires absolute identity for each and every element set forth in the claimed invention. *See Trintec Indus. Inc. v. Top-U.S.A. Corp.*, 63 U.S.P.Q.2d 1597 (Fed. Cir. 2002). Additionally, the cited prior art reference must be enabling, thereby placing the allegedly disclosed matter in the possession of the public. *In re Brown*, 329 F.2d 1006, 1011, 141 U.S.P.Q. 245, 249 (C.C.P.A. 1964). Thus, the prior art reference must adequately describe the claimed invention so that a person of ordinary skill in the art could make and use the invention.

Appellants respectfully submit that the pending claims are patentable over the cited reference because the cited reference fails to disclose or suggest many of the recitations of the pending claims.

II. The Section 102 Rejections

A. The Rejection of Independent Claim 1

As stated above, independent Claim 1 stands rejected under 35 U.S.C. § 102 as being unpatentable over Jacobson. Independent Claim 1 recites:

> A method for managing a security policy for one or more users in a network, comprising:
>
> a) running a policy management program on a computer in communication with the network;
>
> b) enabling creation of a security policy document in a portable representation language using the policy management program, including selection and inclusion in the security policy document of a plurality of data elements for communicating the security policy to the one or more users **and of at least one data element for implementing the security policy on computer systems in the network**;
>
> c) enabling the one or more users on the network to view the security policy document using the plurality of data elements for communicating the

> security policy to the one or more users included in the security policy document; and
>
> d) receiving electronic data relevant to user viewing of the security policy document using the policy management program. (emphasis added)

Appellants submit that at least the highlighted recitations are clearly not disclosed or suggested by Jacobson for at least the reasons discussed herein.

In rejecting independent Claim 1, the Final Action cites to portions of columns 2, 10, 11 and 19 of Jacobson. Final Action, p. 4. However, the only portion of Jacobson added responsive to the amendments to Claim 1 to add the highlighted portions of Claim 1 are at column 19, lines 19-32. Furthermore, in response to Appellants' arguments regarding patentability of Claim 1, the Response to Arguments section of the Final Action states that the policy document, the data elements for communicating the security policy **and** at least one data element for implementing the security policy on a computer are taught by the excerpt at column 19, lines 19-32. Final Action, p. 2. The paragraph including this excerpt, in its entirety, reads as follows:

> Software resources include software listings and updates, guidelines for proper use including email etiquette, and netiquette training, Internet information and personal safety training, optional registration of an encryption private or public key with the system, a listing of the organization's approved and licensed software, software downloading guidelines and approved procedures, tech support for user's questions Registering newly downloaded software to the system, management approved trialware, shareware and others for review by the organization, operations and support information, regulation, policy, and Freedom of Information Act materials, information explaining how the system works including product support and services, telephony, text-based support, and in-house support options, a simple do & don't security module for non technical activity, and online safety information. (Jacobson, Col. 19, lines 17-32.)

Even assuming the presentation of access to information on security policies is disclosed by this excerpt, there is no disclosure or even a suggestion of distinct data elements for implementing the security policy on a computer. As described, for example, at paragraph 47 of the present specification, these data elements, for example, contain "the platform controls that link the written security policy to the mechanism for communicating the security policy to the computer systems 26 on the various platforms" and "the technical controls that link the written security policy to the mechanism for enforcing the security policy on the computer systems." Such data elements are not disclosed or even suggested by the excerpt relied on from Jacobson. In fact, the only statement in the Remarks section of the Final

Action that appears to even relate to the distinct data elements recitations, as opposed to a portable representation language, is "the new policy is automatically added and the software resources includes [sic] updates." Final Action, p. 2. Appellants respectfully submit that such a generalized characterization fails to disclose or suggest the recited data elements of independent Claim 1.

In addition, while an HTML type provision of information to remote locations executing on browser is inferred in Jacobson, it does not follow that the HTML would disclose or suggest the "security policy document" of Claim 1. Instead, it merely indicates that screen display information, which may include information related to a "policy," may be provided to remote locations in an HTML form. The "policy training module" and other modules of Jacobson are not described as creating a specific "security policy **document**" that contains such HTML form information. Instead, such displays may be standard page or frame displays saved on a system, text information stored in a database or the like and extracted by the policy training module and/or various known other ways to create HTML pages and the like.

Furthermore, the Final Action appears to not even distinguish between the recited policy management **program** and the recited policy **document** of Claim 1 in applying Jacobson. The "network security policies stored in the database" of Jacobson, while arguably a document, are not even alleged in the Final Action as disclosing the particulars of "a security policy document" as recited in Claim 1. Neither does Jacobson appear to discuss "enabling creation" of such stored policies by the described policy compliance monitor 110 or effectiveness module 120 (shown as coupled to the policy repository 125 of Figure 1 of Jacobson).

Accordingly, independent Claim 1 is patentable over Jacobson for at least the reasons discussed above. Furthermore, Appellants submit that dependent Claims 2-10 are patentable at least per the patentability of independent Claim 1, from which they depend. Therefore, Appellants respectfully request reversal of the rejections with respect to Claim 1 and the claims that depend therefrom for at least the reasons discussed herein.

B. The Rejection of Independent Claim 11

Independent Claim 11 recites technical controls "for implementing the security policy on at least one first computer." In rejecting Claim 11, the Final Action asserts that these

recitations are disclosed by Jacobson, Col. 2, lines 3-18, Col. 10, line 57 to Col. 11, lines 3 and Col. 6, lines 47-57. Final Action, pp. 5-6. However, at most these sections refer to "compliance actions" that may include "implementing a different security policy." However, as stated in these sections of Jacobson, a "security policy" is identified as "a set of rules designed to limit an organization's risk and liability." *See*, Jacobson, Col. 10, lines 66-67. Implementing is described in Jacobson as training users on policy and, more particularly, using that training as a way to develop policies. *See*, Jacobson, Col. 5, lines 36-50. Thus, Appellants' submit that the portions of Jacobson relied on in rejecting Claim 11 (and Claim 1), while they recite "implementing a different security policy," do not disclose or even suggest creation of a security policy **document** including at least one **data element** for implementing the security policy on **computer systems**. Instead, they, at most, suggest changing rules for **users** and training **users** on those new rules to encourage compliance by increased user appreciation of the "organization's risk and liability." *See*, Jacobson, Col. 10, line 67. Accordingly, Appellants respectfully request reversal of the rejections with respect to Claim 11 and the claims that depend therefrom for at least the reasons discussed herein and for reasons substantially the same as discussed above with reference to corresponding recitations of independent Claim 1.

In addition, Claim 11 also includes the recitation of "enabling creation of a security policy document ... by enabling selection of security policies from a set of options." The Response to Arguments section of the Final Action asserts that these recitations are taught by the same section of Jacobson (column 19, lines 19-32) as reproduced above. Final Action, p. 3. However, Appellants can find no discussion or suggestion of enabling creation of a security policy document by enabling selection of security policies from a set of options anywhere in this excerpt. Accordingly, Appellants also respectfully request reversal of the rejections with respect to Claim 11 and the claims that depend therefrom for at least these additional reasons.

C. The Rejection of Independent Claims 26 and 51

Independent Claim 26, like Claims 1 and 11, recites a distinct program and "security policy document." Claim 26 also recites configuring the security policy document to create both "a human-readable security policy document" and a "machine-readable security policy document containing technical controls readable by" a computer. In rejecting Claim 26, the

Response to Arguments Section of the Final Action simply states "the applicant arguments are directed to similar limitations as addressed above." Final Action, p. 3. The only section of Jacobson "addressed above" was the excerpt at column 19, lines 19-32 discussed above with reference to the rejections of Claims 1 and 11. Appellants agree that, while the wording of the recitations are different in Claim 26, the arguments above discussing what the excerpt of Jacobson discusses similarly establish that this excerpt does not include an anticipatory disclosure of such particular recitations of inclusion of human and machine information in a security policy document to provide security policy management "for one or more **users and** one or more first **computers** in a network" as recited in Claim 26 (emphasis added). Independent Claim 51 includes corresponding recitations related to a "program for creating a security policy document in both human-readable and machine-readable formats." Accordingly, Appellants respectfully request reversal of the rejections with respect to independent Claims 26 and 51 and the claims that depend therefrom for at least the reasons discussed herein.

III. Many of the Dependent Claims are Separately Patentable

As stated above, the dependent claims are also all rejected under 35 U.S.C. § 102(e) as being unpatentable over Jacobson. Many of the dependent claims are separately patentable over the cited art.

A. Claims 16 is Separately Patentable

Claim 16 recites "distributing detect rules" to at least one first computer. The rejection of Claim 16 at page 6 of the Final Action is based on the following excerpt from Jacobson:

> performed by the policy training module 105 in performing the generating a network security policy step represented by block 220 according to an embodiment of this invention;

Jacobson, Col. 8, lines 7-10. Appellants submit that there is no discussion related to distributing detect rules in this excerpt and Claim 16 is separately patentable for at least these additional reasons. Accordingly, Appellants also respectfully request reversal of the rejections with respect to Claim 16 for at least these additional reasons.

B. Claims 18 and 19 are Separately Patentable

Claims 18 and 19 include recitations related to distributing and converting technical controls. The rejections of Claims 18 and 19 at page 6 of the Final Action are based on the following excerpt from Jacobson:

> The network policy compliance actions may include electronically implementing a different network security policy selected from network security policies stored in the database, generating policy effectiveness reports, and providing a retraining module to network users.

Jacobson, Col. 2, lines 14-19. Appellants submit that implementing a different security policy does not disclose distributing or converting technical controls or even, as discussed above, teach technical controls. Accordingly, Claims 18 and 19 are separately patentable for at least these additional reasons. Accordingly, Appellants also respectfully request reversal of the rejections with respect to Claims 18 and 19 for at least these additional reasons.

C. Claims 53-56 are Separately Patentable

Claims 53-56 include various recitations related to particular data elements and platform control elements for different operating system platforms. The rejections of Claims 53-56 at pages 9-10 of the Final Action are based on the excerpt from column 19 reproduced above and a portion of the following excerpt from Jacobson:

> The Internet and computer networks allow organizations to store applications and information on central servers, waiting to be called up and manipulated from any location. Networks allow people greater access to files and other confidential information. Global networks, including the Internet, and remote access increase the vulnerability of corporate data, increase the risk of information leaks, unauthorized document access and disclosure of confidential information, fraud, and privacy.

Jacobson, Col. 1, lines 11-19. Appellants submit that the recitations of these claims are clearly not disclosed in the excerpt from column 1 of Jacobson. As discussed above, the excerpt from column 19 fails to disclose the plurality of data elements. Accordingly, it also necessarily fails to disclose the particular related details recited in Claims 53-56. Accordingly, Appellants also respectfully request reversal of the rejections with respect to Claims 53-56 for at least these additional reasons.

III. Conclusion

In light of the above, Appellants request reversal of the rejections of the claims, allowance of the claims and passing of the application to issue.

It is not believed that an extension of time and/or additional fee(s) are required, beyond those that may otherwise be provided for in documents accompanying this paper. In the event, however, that an extension of time is necessary to allow consideration of this paper, such an extension is hereby petitioned for under 37 C.F.R. §1.136(a). Any additional fees believed to be due in connection with this paper may be charged to Deposit Account No. 50-0220.

Respectfully submitted,

Robert W. Glatz
Registration No. 36,811
Attorney for Appellants

Myers Bigel Sibley & Sajovec, P.A.
P. O. Box 37428
Raleigh, North Carolina 27627
Telephone: (919) 854-1400
Facsimile: (919) 854-1401

Certificate of Mailing under 37 CFR 1.8

I hereby certify that this correspondence is being deposited with the United States Postal Service with sufficient postage as first class mail in an envelope addressed to: Mail Stop Appeal-Brief Patens, Commissioner for Patents, PO Box 1450, Alexandria, VA 22313-1450 on July 11, 2006.

Carey Gregory

APPENDIX A - Claims Appendix

1. (Previously presented) A method for managing a security policy for one or more users in a network, comprising:

a) running a policy management program on a computer in communication with the network;

b) enabling creation of a security policy document in a portable representation language using the policy management program, including selection and inclusion in the security policy document of a plurality of data elements for communicating the security policy to the one or more users and of at least one data element for implementing the security policy on computer systems in the network;

c) enabling the one or more users on the network to view the security policy document using the plurality of data elements for communicating the security policy to the one or more users included in the security policy document; and

d) receiving electronic data relevant to user viewing of the security policy document using the policy management program.

2. (Original) The method of claim 1, further comprising verifying a degree of user compliance with the security policy by using the policy management program to assess the received data.

3. (Original) The method of claim 2, wherein the received data includes a timestamp denoting the time a user acknowledges viewing of the security policy document.

4. (Original) The method of claim 2, wherein the received data includes quiz results indicative of the user comprehension of the viewed security policy document.

5. (Original) The method of claim 1, wherein enabling the creation of the security policy document comprises enabling selection of security policies from a set of options.

6. (Original) The method of claim 5, wherein the security policies selected from the set of options reside in a library in communication with the policy management program.

7. (Original) The method of claim 1, wherein enabling the users on the network to view the security policy document comprises enabling pre-selection of a group of users to view the security policy document.

8. (Original) The method of claim 1, further comprising electronically providing a quiz to assess user comprehension of the viewed security policy document.

9. (Original) The method of claim 1, wherein enabling the creation of the security policy document further comprises enabling creation of a quiz associated with the security policy document.

10. (Original) The method of claim 8, wherein the received data includes user responses to the quiz.

11. (Original) A method for managing a security policy for one or more first computers in a network, comprising:

a) running a software program on a second computer in communication with the network;

b) enabling creation of a security policy document using the software program by enabling selection of security policies from a set of options; and

c) automatically configuring the security policy document to provide one or more technical controls for implementing the security policy on at least one first computer.

12. (Original) The method of claim 11, wherein the security policies selected from the set of options reside in a library in communication with the software program.

13. (Original) The method of claim 11, wherein two of the first computers operate in accordance with different operating systems.

14. (Original) The method of claim 11, wherein the technical controls comprise a format interpretable by at least one first computer.

15. (Original) The method of claim 11, wherein the security policy document is represented by a markup language.

16. (Original) The method of claim 11, further comprising distributing detect rules to at least one first computer.

17. (Original) The method of claim 16, further comprising electronically notifying an administrator when at least one first computer is out of compliance.

18. (Original) The method of claim 11, further comprising distributing the one or more technical controls to at least one first computer.

19. (Original) The method of claim 18, further comprising running a second software program on at least one first computer to allow at least one first computer to interpret the distributed technical controls.

20. (Original) The method of claim 19, wherein the second software program uses metacommands to convert the technical controls into instructions interpretable by an operating system running on at least one first computer.

21. (Original) The method of claim 11, further comprising receiving data relevant to compliance of at least one first computer with the one or more technical controls using the software program.

22. (Original) The method of claim 21, further comprising assessing the received data using a third software program.

23. (Original) The method of claim 22, wherein the third software program comprises a security management program.

24. (Original) The method of claim 21, further comprising verifying a degree of compliance of at least one first computer with the one or more technical controls by using the software program to assess the received data.

25. (Original) The method of claim 24, wherein the received data comprises compliance score data.

26. (Original) A method for managing a security policy for one or more users and one or more first computers in a network, comprising:

a) running a software program on a second computer in communication with the network;

b) creating a security policy document using the software program; and

c) automatically configuring the security policy document to create (i) a human-readable security policy document, and (ii) a machine-readable security policy document containing technical controls readable by at least one first computer.

27. (Original) The method of claim 26, further comprising allowing the users to view the human-readable security policy document via the network.

28. (Original) The method of claim 27, wherein allowing the users to view the human-readable security policy document comprises pre-selecting a group of users to view the security policy document.

29. (Original) The method of claim 27, further comprising electronically receiving data relevant to user viewing of the security policy document.

30. (Original) The method of claim 29, wherein the received data includes a timestamp denoting the time a user acknowledged viewing the security policy.

31. (Original) The method of claim 29, further comprising verifying a degree of user compliance with the security policy by using the software program to assess the received data.

32. (Original) The method of claim 31, wherein the received data includes quiz results indicative of the user comprehension of the viewed security policy document.

33. (Original) The method of claim 26, wherein creating the security policy document comprises selecting security policies from a set of options.

34. (Original) The method of claim 33, wherein the security policies selected from the set of options reside in a library in communication with the software program.

35. (Original) The method of claim 26, wherein the human-readable security policy document includes a quiz to test user comprehension of the security policy document.

36. (Original) The method of claim 26, further comprising electronically providing a quiz to assess user comprehension of the viewed security policy document.

37. (Original) The method of claim 26, wherein enabling the creation of the security policy document further comprises enabling creation of a quiz associated with the security policy document.

38. (Original) The method of claim 26, further comprising distributing the machine-readable security policy document to at least one first computer to implement the security technical controls thereon.

39. (Original) The method of claim 38, further comprising running a second software program on at least one first computer to allow at least one first computer to interpret the distributed technical controls.

40. (Original) The method of claim 39, wherein the second software program uses metacommands to convert the technical controls into instructions interpretable by an operating system running on at least one first computer.

41. (Original) The method of claim 38, further comprising receiving data relevant to compliance of at least one first computer with the technical controls using the software program.

42. (Original) The method of claim 41, further comprising assessing the received data using a third software program.

43. (Original) The method of claim 42, wherein the third software program comprises a security management program.

44. (Original) The method of claim 41, further comprising verifying a degree of compliance of at least one first computer with the technical controls by using the software program to assess the received data.

45. (Original) The method of claim 44, wherein the received data comprises compliance score data.

46. (Original) The method of claim 26, wherein two of the first computers operate in accordance with different operating systems.

47. (Original) The method of claim 26, wherein the technical controls comprise a format interpretable by at least one first computer.

48. (Original) The method of claim 47, wherein the security policy documents is represented by a markup language.

49. (Original) The method of claim 26, further comprising distributing detect rules to at least one first computer.

50. (Original) The method of claim 49, further comprising electronically notifying an administrator when at least one first computer is out of compliance.

51. (Original) A system for managing a security policy for one or more users and for one or more first computers in a network, comprising:

a) a first device containing a first program for creating a security policy document in both human-readable and machine-readable formats; and

b) a second device in communication with the first device and containing a second program for monitoring the security compliance of at least one first computer; wherein at least one first computer contains a third program for receiving the machine-readable format of the security policy document.

52. (Previously presented) The method of claim 1, wherein the portable representation language comprises a structured data representation language.

53. (Previously presented) The method of claim 52, wherein the plurality of data elements for communicating the security policy to the one or more users include a policy statement element, a policy commentary element and an example element and wherein the at least one data element for implementing the security policy on computer systems in the network includes a platform control element specific to a platform type corresponding to an operating system of ones of the computer systems.

54. (Previously presented) The method of claim 1, wherein enabling creation of the security policy document comprises enabling creation of a plurality of security policy documents associated with the security policy, ones of the security policy documents including data elements for different platform types corresponding to operating systems of the computer systems in the network.

55. (Previously presented) The method of claim 11, wherein the one or more first computers in the network comprises a plurality of first computers, ones of which are different platform types corresponding to operating systems of the respective first computers, the

method further comprising automatically configuring the security policy document to include a plurality of platform controls, ones of which include commands for enforcing the security policy on the different platform types corresponding to operating systems of the plurality of first computers in the network.

56. (Previously presented) The method of claim 11, wherein the one or more first computers in the network comprises a plurality of first computers, ones of which are different platform types corresponding to operating systems of the respective first computers and wherein enabling creation of a security policy document comprises enabling creation of a plurality of security policy documents associated with the security policy, the method further comprising automatically configuring respective ones of the security policy documents to include a platform control that includes commands for enforcing the security policy on a corresponding one of the different platform types.

APPENDIX B – EVIDENCE APPENDIX

(NONE)

APPENDIX C – RELATED PROCEEDINGS

(NONE)